2016 春 情報セキュリティスペシャリスト 全国統一公開模試 講評と採点基準

2016 年 3 月 22 日 (株)アイテック IT 人材教育研究部

■ 全体講評

今回の公開模試における午後Ⅰ，午後Ⅱ試験の平均点は，午後Ⅰが 35.7 点，午後Ⅱが 34.9 点でした。問題別では，午後Ⅰの問 1 が 18.9 点，問 2 が 18.0 点，問 3 が 17.6 点で，問 1 の平均点が，わずかながら最も高くなりました。また，午後Ⅱは，問 1 が 31.4 点，問 2 が 38.7 点で，かなりの差が見られました。2015 年秋期の公開模試では，午後Ⅰの平均点が 36.7 点，午後Ⅱの平均点が 31.9 点でしたから，平均点で評価すると，午後Ⅰが低く，午後Ⅱが高くなりました。

採点結果から受けた印象としては，記述式の設問では，下線部にだけ注目しそれに関することを取り上げて解答を作成していたり，設問で指示されていることにあまり注意せず，各自がもち合わせている知識や先入観などに基づいて解答を作成していたりすると思われる答案が多く見られました。合格するためには，問題の記述内容や設問の指示に従って，素直に答案を作成していくことが必要です。こうした事項については，本番の試験に向けて必ず改善していってほしいと思います。また，記述式の問題においては，それぞれの設問で求める解答は基本的に一つの内容を答えさせるように条件が付けられています。このため，主語と述語，あるいは目的語は何かなどを明確にした上で解答を作成するようにしましょう。なお，問題によっては，設問で具体的に述べよと指示されている場合があります。こうしたケースでは，例えば，必要最小限の範囲に対してだけ権限を与えるなどと解答しても，それでは具体的と見なされません。権限が与えられるべき範囲を問題の記述から導き出し，それを具体的に表現することが必要です。

次に，問題ごとの選択状況を紹介しておきます。午後Ⅰ試験は，問 1（セキュアプログラミング）の選択者が 9.3%，問 2（迷惑メール対策）が 45.8%，問 3（クラウドサービス利用における認証方式の検討）が 44.9%で，多くの受験者が問 2 と問 3 を選択していました。なお，本試験の午後Ⅰで出題される問題数は 3 問ですから，各自が得意とする分野の問題をいち早く見つけ出し，それに集中して取り組むことが必要になると思われます。例えば，得意分野の問題で 40 点近くの点数を獲得できれば，もう一つの問題で 20 点強を得点するだけで，午後Ⅰ試験はクリアすることができます。しかし，このようなことが可能になるには，問題の記述内容を十分に把握できるだけの知識が，まず必要とされます。本番の試験日までの期間で，より一層のレベルアップを図るようにしましょう。

午後Ⅱ試験は，問 1（インターネットサービスのセキュリティ）の選択者が 52.3%，問 2（サービス利用におけるセキュリティの見直し）が 47.7%で，選択者数は，ほぼ半々という結果でした。午後Ⅱ試験は，様々なセキュリティ分野の知識が問われる総合問題になることが多いので，できるだけ各自が得意とする分野から構成されている問題を選択するとよいでしょう。また，試験センターでは「試験結果に問題の難易差が認められた場合には，基準点の変更を行うことがあります」としています。このため，午後Ⅱ試験においては，問 1 と問 2 の難易差をあまり気にせず，一度選択すると決めた問題を最後までやり遂げることが大切です。問題選択に迷ってしまうと，2 問とも手をつけ，かえって失敗することになってしまいます。

午後Ⅰ，午後Ⅱ試験の記述式問題の多くは，問題文の中に解答を導くためのヒントが記述されています。一定の知識レベルに到達していれば，問題文で記述された内容を基にして正解を導き出すことができます。しかし，受験者によっては問題文の記述内容をそのまま引用して解答を作成している例も多く見られます。単なる引用では正解になることは極めて少ないので，設問で問われていることを十分に確認し，問題の記述内容と照らし合わせながら論理的に考えていくようにしましょう。

試験当日は集中力，精神力，体力の勝負になります。必ず合格するという強い意志をもって，午後Ⅱ試験の最後まで全力を出し切り（あきらめず）問題に取り組んで，ぜひ合格するようにしましょう。

＜午後Ⅰ＞

問1 セキュアプログラミング

【採点基準】

[設問1]

ア～カは，解答例どおりに対し各 3 点。

[設問2]

(1) 解答例どおりに対し 3 点。その他は 0 点。

(2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は 0 点。

[設問3]

(1) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は 0 点。

(2) 解答例どおりに対し 4 点。その他は 0 点。

(3) キーワードは，解答例どおりに対し 3 点。その他は 0 点。結果は，解答例と同様の趣旨が適切に指摘されているものに対し 4 点。その他は 0 点。

（4）追加するコードは，解答例どおりに対し 4 点。その他は 0 点。場所は，解答例どおりに対し 2 点。その他は 0 点。

【講評】

平均点は 18.9 点（平均正答率は 37.7%）で，午後 I の 3 問の中では，最も高い点数でした。Java を理解している受験者が主に選択していたことなどが，その要因と考えられます。

設問 1 の穴埋め問題は，空欄オを除き，まずまずの正答率だったと思います。

設問 2 (2)は，Java において親プロセスが常駐する際，ガーベジコレクションを実行できる条件を問うものでしたが，正答率は低かったようです。少し考えにくい面もあったかもしれませんが，できるだけ問題文を丁寧に読んで，どのような条件の下で考えるものかを見極めていくようにしましょう。

設問 3 は，まずまずの正答率だったと思います。

午後 I 試験の出題数は 3 問ですから，本番の試験でもセキュアプログラミングや，HTML などが含まれる問題を選択せざるを得ないケースが考えられます。その際の準備としては，IPA が公開している「セキュア･プログラミング講座」，「安全なウェブサイトの作り方」，「安全な SQL の呼び出し方」，「セキュアな Web サーバの構築と運用」などの資料を事前に学習しておくことが必要です。しかし，これらの資料を短期間でマスターすることは大変ですから，長期的に取り組んでいく方がよいでしょう。また，Java，C++，ECMAScript などのプログラミング言語に加え，HTML で記述されたコードは，できるだけ理解できるようにしておきましょう。

問2 迷惑メール対策

【採点基準】

［設問1］

（1）a ～ e は，解答例どおりに対し各 2 点。

（2）解答例と同様の趣旨（当該 ISP 以外のメールサービスを利用するというキーワード）が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問2］

（1）f，g は，解答例どおりに対し各 2 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。指摘内容が今一歩のものは 3 点。その他は 0 点。

（3）解答例と同様の趣旨（署名の検証に失敗すること）が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（4）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問3］

（1）h，i は，解答例どおりに対し各 1 点。意味は，解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例どおりに対し 4 点。その他は 0 点。

【講評】

平均点は 18.0 点（平均正答率は 35.9%）で，午後 I の 3 問の中では平均的な点数でした。また，この問題の選択者は 45.8%でしたから，ほとんどの受験者が問 2 を選択していたことになります。

設問 1 (1)の正答率は，全体的に低かったようです。一般に，技術的な用語問題は，正答率が低くなる傾向がありますが，合格を目指すには，様々なセキュリティ知識を習得し，本番の試験に臨むことが必要です。日ごろから一つ一つの積み重ねを大切にしていきましょう。

設問 2 (1)は，メールヘッダの専門知識の問題でしたから，正答率は低かったようです。その半面，(2)の SPF の検証の仕組みや，(4)の送信ドメイン認証において迷惑メールと判定されないケースの問題は，理解している受験者が少しずつ増えているように感じられます。SPF は，メールの受信側が送信側を認証する仕組みです。受信側は，メールアドレスに記載されているドメイン（@ 以降の名前）の DNS サーバに対して SPF レコードを問い合わせ，その結果，得られた IP アドレスと，送信メールサーバの IP アドレスを比較し，両者が一致すれば，メールを受信するという仕組みです。一方，DKIM は，送信するメールに対して送信側でディジタル署名を付与し，受信側ではその署名を検証して，メールの送信者の真正性と，メールの完全性を確認するものです。このため，メールヘッダの Received フィールドなどを署名対象にすると，メールを中継するメールサーバによって情報が付け加えられ，署名を送信者の公開鍵で復号した値と，受信側でメールヘッダとメール本文から求めたハッシュ値が一致しなくなるので，署名の検証に失敗してしまいます。こうした基本的な知識については，しっかり理解するようにしましょう。

設問 3 は，まずまずの正答率だったと思います。FW のフィルタリングルールについては，問題の条件を考慮し，正確に記述するようにしましょう。

問3 クラウドサービス利用における認証方式の検討

【採点基準】

［設問1］

（1）a は，解答例どおりに対し 3 点。その他は 0 点。

（2）b は，解答例と同様の趣旨が適切に指摘されてい

るものに対し 6 点。その他は，基本的に 0 点。

［設問2］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）番号は，解答例どおりに対し 2 点。理由は，解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問3］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問4］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例どおりに対し 3 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

【講評】

平均点は 17.6 点（平均正答率は 35.1%）で，午後 I の 3 問の中では最も低くなりました。また，この問題の選択者は 44.9%で，問 2 とほぼ同数でした。

設問 1 (1)，(2)とも，正答率は低かったようです。(2)はパスワード破りを行う手法に関する問題です。パスワードをハッシュ化した場合，ハッシュ値から元のパスワードを求めることは基本的にできません。そこで，攻撃者は，全ての組合せのパスワード候補のハッシュ値を求めたテーブルをあらかじめ作成し，窃取したハッシュ化パスワードとテーブルを照合して，一致したハッシュ値に対応したものが元のパスワードであるという手口をよく用います。これまでの試験でも類似のものが出題されていますので，よく理解しておきましょう。

設問 2 (1)の正答率は高かった半面，(2)の正答率は低かったと思います。TCP の特徴は，IP アドレスを詐称すると，コネクションを確立できないという点です。なお，TCP 通信で IP アドレスを詐称すると，SYN Flood などの DoS 攻撃に悪用されることになります。

設問 3 (1)は，ワンタイムパスワードがリプレイ攻撃に有効であることを問いましたが，「パスワードがネットワーク上を流れない」や，「ハッシュ値から元のパスワードを復元できない」などの答案が見られました。ログイン時に同じパスワードによって認証を受けないことが，ワンタイムパスワードの特徴です。

設問 4 (1)，(2)の正答率は低かったようですが，(3)の正答率は，想定以上に良かったと思います。

＜午後Ⅱ＞

問1　インターネットのセキュリティ

【採点基準】

［設問1］

（1）a，b（完答），c ～ e（完答）ともに，解答例どおりに対し各 4 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（4）f は，解答例どおりに対し 4 点。

［設問2］

（1）g ～ j は，解答例どおりに対し各 3 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点。

（4）k，l は，解答例どおりに対し各 3 点。

（5）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問3］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 8 点。指摘内容が今一歩のもの（条件が不足しているもの）は 4 点。その他は 0 点。

（4）m，n は，解答例どおりに対し各 2 点。なお，n については，MX レコードを問い合わせると，A レコードも追加情報として回答されるので，MX だけでも正解にしています。

［設問4］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点。

【講評】

問 1 の平均点は 31.4 点で，問 2 よりも 7.3 点低い結果でした。一部の受験者は，内容のしっかりした答案を作成し，高得点をあげていました。本番の試験に向けて十分な準備ができていると感じられます。

設問 1 (2)の正答率は良かった半面，(1)，(4)の正答率は低かったようです。(1)，(4)は，問題文に条件が記述されていますので，条件に合うようにルールを追加したり，計算したりすることが必要です。なお，(2)は，午後

I 問 3 設問 2 (2)の裏返しの問題です。UDP では IP アドレスを詐称しやすいことには着目できても，TCP では詐称できない理由について，的確に答案が作成できていませんでした。この際，TCP と UDP の違いなどをよく整理しておきましょう。

設問 2 では，(2)，(3)の正当率が低かったと思います。XSS 攻撃には，反射型のほかに格納型（セカンドオーダ XSS）などもあります。Web サイトのセキュリティについては，よく理解されていると思いますが，攻撃方法も多様化しています。最新の動向も含め，できるだけ幅広く理解しておくとよいでしょう。

設問 3 の正答率は，全体的に低かったようです。(1)は，ウイルスに感染した場合の復旧対策の面から解答することが必要です。下線部だけに着目するのではなく，問題の流れの中から，適切な答案を作成するように心掛けましょう。(3)も，条件の抽出が難しいものでしたが，問題の条件を整理しながら，論理的に考えていくことが必要です。

設問 4 の正答率も，全体的に低かったようです。(1)は，ハッシュ関数の衝突を利用し，証明書 A とハッシュ値が同じになる証明書 X を作成できれば，証明書 A にある CA のディジタル署名を，証明書 X にもってくるだけで，偽の証明書を作成できるということがポイントです。(2)は，設問で問われていることに対して素直に答えていくことが必要です。

問2 サービス利用におけるセキュリティの見直し

【採点基準】

［設問1］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問2］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点。

（3）解答例どおりに対し 6 点。その他は 0 点。

［設問3］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点

（3）解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点。

（4）非効率な点，見直しの内容とも，解答例と同様の趣旨が適切に指摘されているものに対し各 4 点。その他は，基本的に 0 点。

（5）解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点。

［設問4］

（1）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨が適切に指摘されているもの（二要素認証を突破する方法が正しく指摘されているもの）に対し 8 点。その他は，基本的に 0 点。

（4）解答例どおりに対し 4 点。その他は 0 点。

【講評】

問 2 の平均点は 38.7 点で，問 1 よりも 7.3 点高くなりました。問 1 と同様に，一部の受験者は，内容のしっかりした答案を作成し，高得点をあげていました。

設問 1 は，全体的に正答率が低かったと思います。(2)では，設問で問われていることを確認し，SSO における通信制御装置の動作を，図 3 などを確認しながら丁寧に答えていくことが必要です（認証済みの利用者に対しては，認証処理を行わず，HTTP リクエストを中継すること）。(3)は，TLS サーバ機能に続いて WAF 機能を動作させる理由を問うているにもかかわらず，表 2 の WAF 機能を述べただけの答案も散見されました。各設問に対しては，丁寧に答えていくようにしましょう。

設問 2 も，設問 1 と同様に，正答率は低かったようです。午後Ⅱ問題は，記述内容が複雑化していることが多いので，まず，問題文を丁寧に読み砕いていった上で解答を作成するように心掛けてください。

設問 3 は，全体的に正答率が高かったようです。スマートフォンのセキュリティ対策などに対する理解は，かなり進んでいるように思われます。

設問 4 (1)，(2)の正答率は高かった半面，(3)，(4)の正答率は低かったと思います。二要素認証（二段階認証）は，同じ端末から認証情報を入力することが必要です。

なお，問 1，問 2 に共通する事項ですが，問題文を表面的にしか読み取っていない，問題の条件設定がどのようになっているかなどの把握が十分になされていない，自身の知識だけから安易に解答を作成しようとする傾向が強いなどといったことが感じられました。本番の試験では，問題文をよく読んで設問で問われていることに対し素直に答えていくようにしましょう。

以上